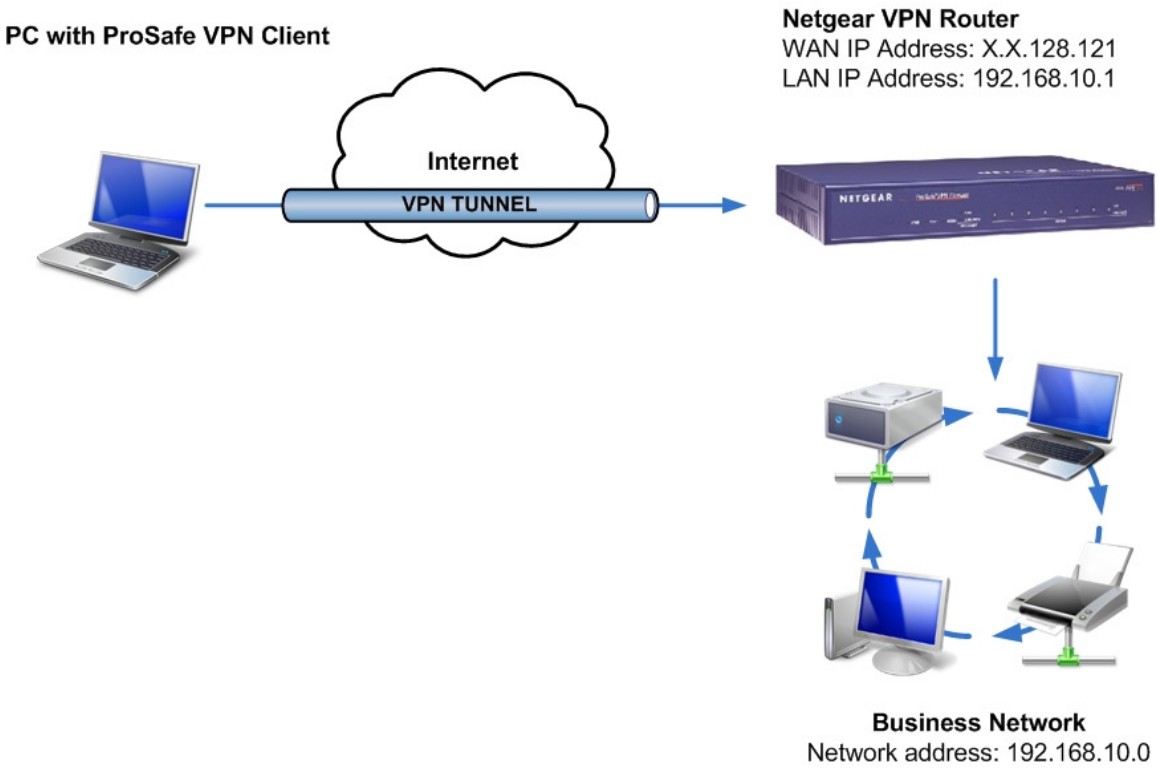
NETGEAR®
Connect with Innovation™

Using certificates as authentication method for VPN connections between Netgear ProSafe Routers and the ProSafe VPN Client

This document describes how to use certificates as an authentication method when establishing a VPN Client-to-Box connection.



Version 2.0

Preliminary notes:

If for your particular deployment you are not using an external CA (Certificate Authority) you will need to create your own CA. Some alternatives on how to achieve this are outlined below, but they are not exclusive to other methods:

1- OpenSSL: http://www.openssl.org,

2- SimpleCA: http://www.vpnc.org/SimpleCA/

3- Microsoft's IIS

For purpose of this document we used:

1- OpenSSL which could be downloaded from the following link: http://www.slproweb.com/products/Win32OpenSSL.html

2- Additionally you will need to install the Perl interpreter. We used ActivePerl which can be downloaded from here: http://www.activestate.com/Products/activeperl/index.mhtml

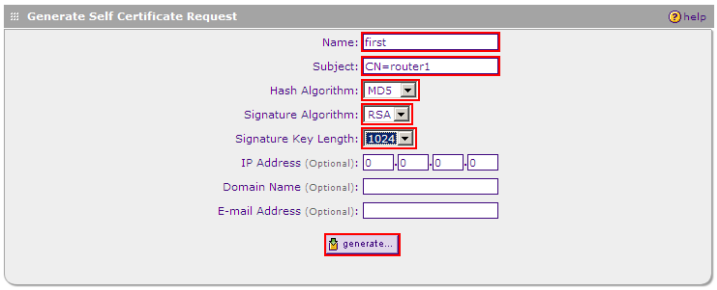
Creating your own Certificate Authority with OpenSSL

1- In first step you need to create your own CA. To do that, follow the instructions documented in here: http://sandbox.rulemaker.net/ngps/m2/howto.ca.html

2- Netgear doesn't support ST relative distinguish name so please edit the openssl.cfg (in the original location and in your new CA folder) to avoid using this parameter.

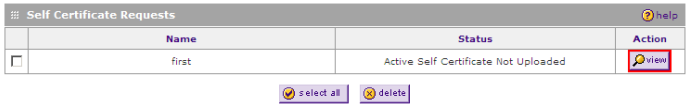
3- From the guide linked above, you need only to execute all the commands up to step 4. The certificate request step and beyond will be handled by the router.

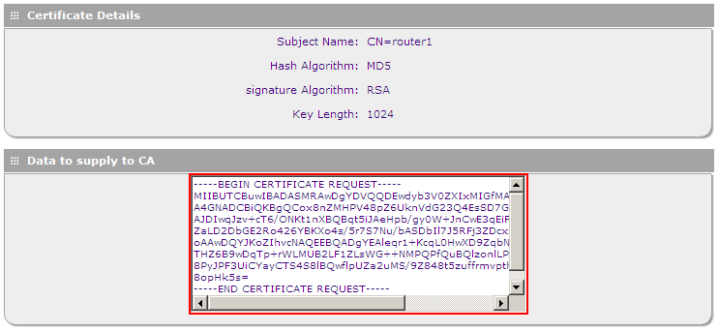
4- Next – please generate Self Certificate Request specifying the following parameters:



1- Name: first
2- Subject: CN=router1
3- Hash Algorithm: MD5
4- Signature Algorithm: RSA
5- Signature Key Length: 1024
6- Click on Generate

5- Click on: "**View**" for generated certificate request to check its values:





Copy all the information from the **Data to supply to CA** field to the text file **router1.csr**

6- Sign your certificate request using your newly created CA:

```
Openssl x509 -req -days 365 -in router1.csr -CA cacert.crt -CAkey cakey.pem -CAcreateserial -
out router1.crt
```

router1.csr – generated self certificate request (router),
cacert.crt – CA certification,
cakey.pem – CA keys,
router1.crt – signed certificate (router).

7- Load CA certificate: "**cacert.crt**" and your signed certificate: "**router1.crt**" on your device. They now should display like this:

Trusted Certificates (CA Certificate) help

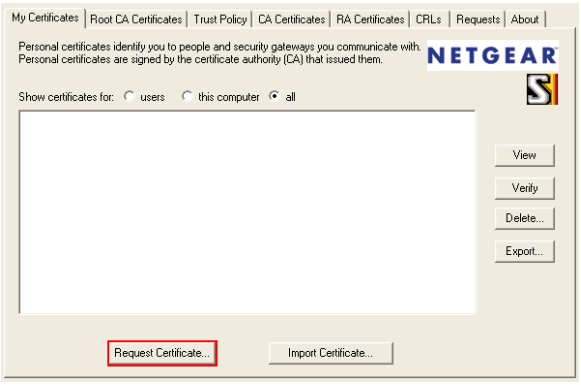
	CA Identity (Subject Name)	Issuer Name	Expiry Time
☐	C=PL, O=Orange PL, OU=IT Support, CN=Supervisor/emailAddress=supervisor@orange.pl	C=PL, O=Orange PL, OU=IT Support, CN=Supervisor/emailAddress=supervisor@orange.pl	Dec 9 17:22:42 2011 GMT

Active Self Certificates help

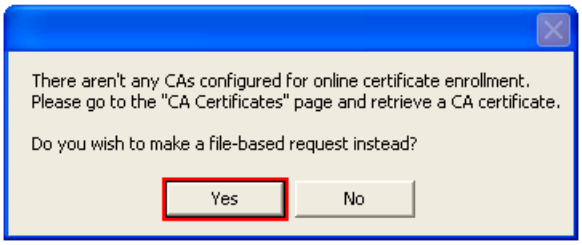
	Name	Subject Name	Serial Number	Issuer Name	Expiry Time
☐	first	CN=router1	89:65:46:12:fb:a3:0f:80	C=PL, O=Orange PL, OU=IT Support, CN=Supervisor/emailAddress=supervisor@orange.pl	Dec 16 13:00:50 2009 GMT

8- Reboot your router.

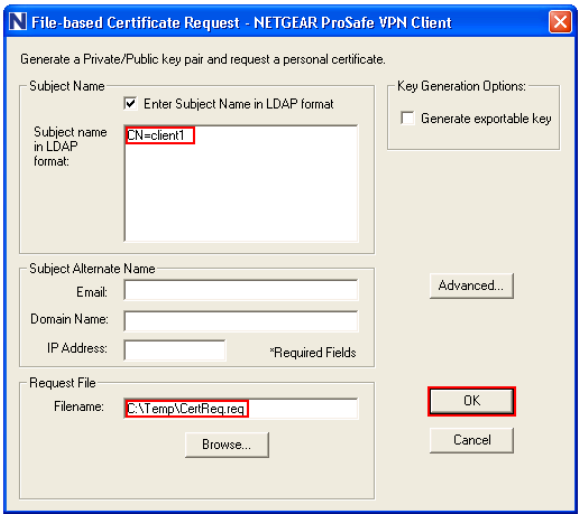
9- Next – generate certificate request using Certificate Manager which is built-in functionality of Netgear's ProSafe VPN Client following these steps:



First, click on Request Certificate.



Then, click on 'Yes' when you get the file-based request prompt.



For last, input the settings like instructed in the screenshot.

Note: Do not change file extension in client software. Change the whole filename after creating a certificate request instead.

10- Rename the generated certificate request from:"**CertReq.req**" to "**client1.csr**".

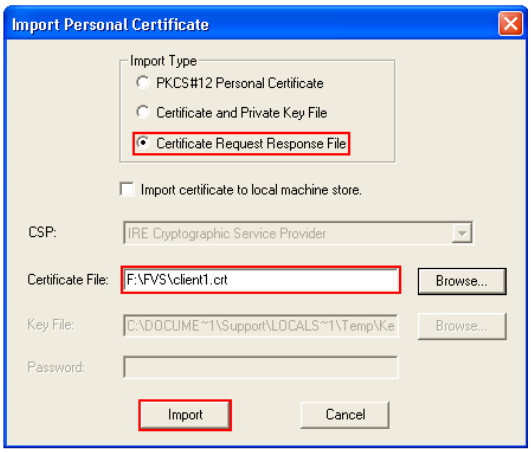
11- Sign your certificate request using your newly created CA:

```
openssl x509 -req -days 365 -in client1.csr -CA cacert.crt -CAkey cakey.pem -CAcreateserial -out client1.crt
```

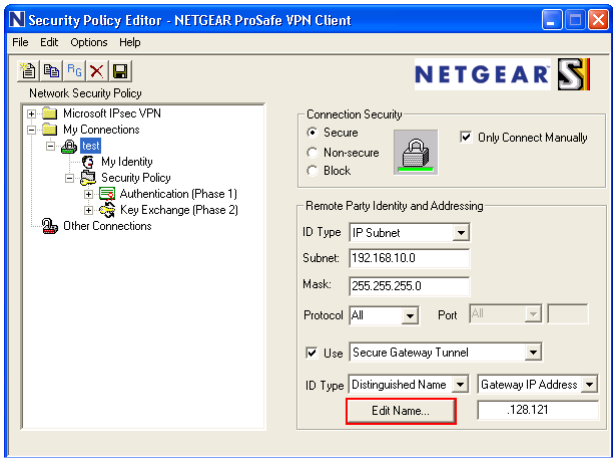
client1.csr – generated self certificate request (client),
cacert.crt – CA certification,
cakey.pem – CA keys,
client1.crt – signed certificate (client).

12- Install CA certificate: "**cacert.crt**" in your system. If you are using Microsoft Windows just select: "Install" from files' context menu.

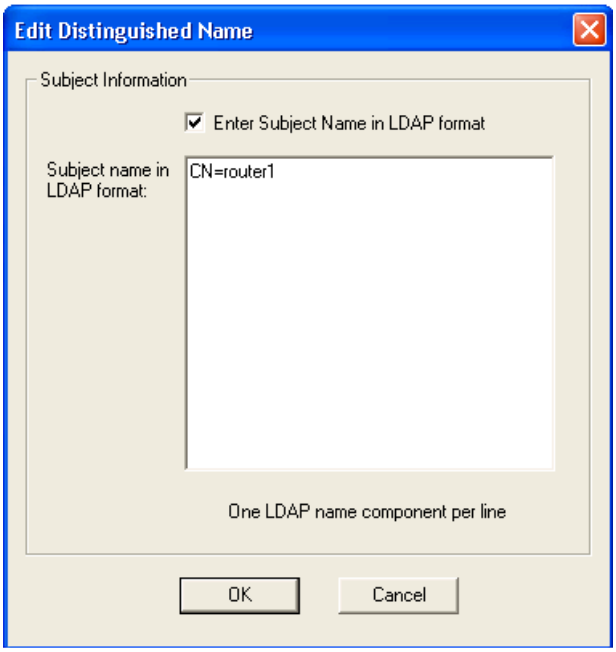
13- Load your signed certificate using the Certificate Manager:



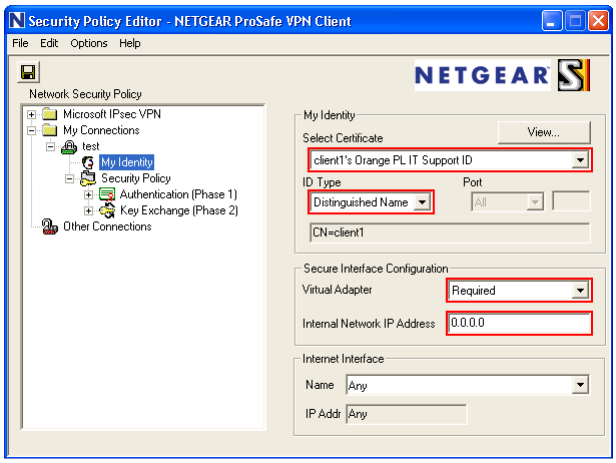
14- Create a new VPN connection according to these steps:



First, input your own details in the same way that is instructed here and click on Edit Name.

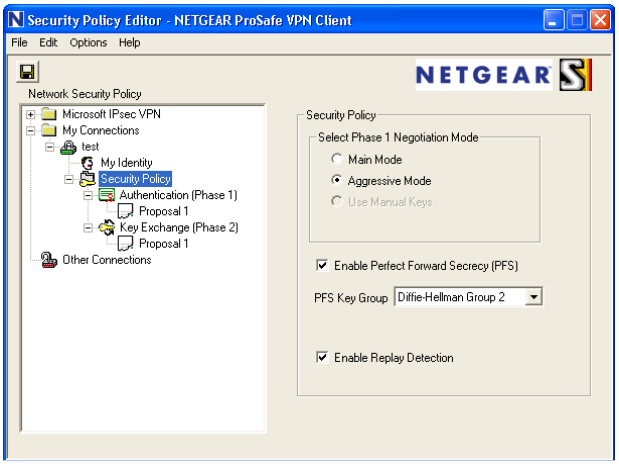


Verify your settings are input correctly in this screen and click on OK.

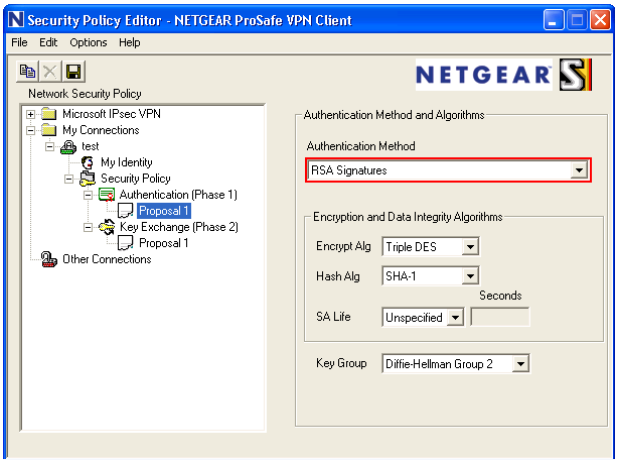


Select the correct certificate, leave the ID Type as Distinguished Name.

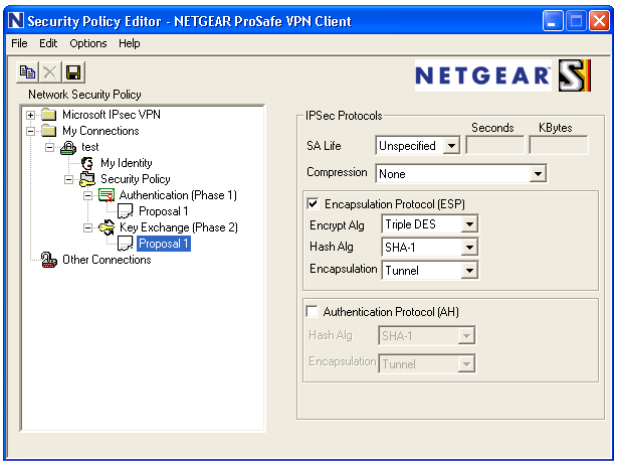
Virtual adapter should be specified as: "Required" to allow using of virtual adapter interface on the client.



In the Security Policy section, verify your settings match those in this screenshot.

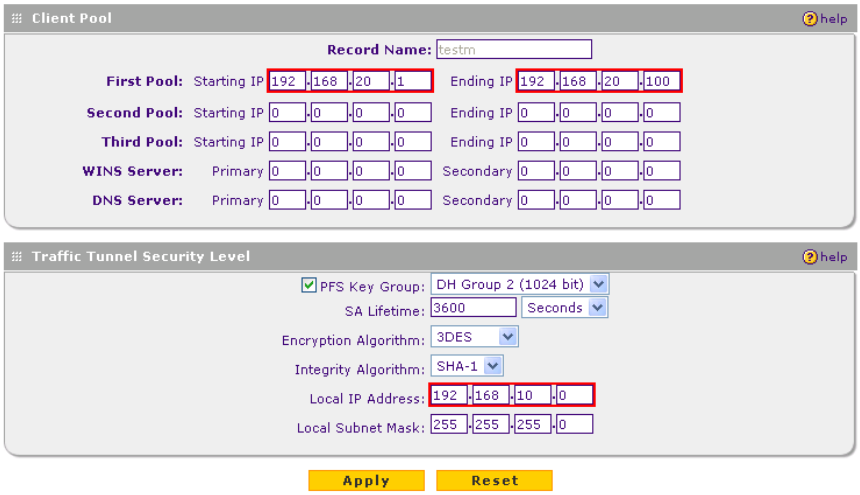


For the "Proposal 1" of the Authentication phase (Phase 1), the Authentication Method should be RSA Signatures.



The Key Exchange Proposal should be correct by default, but check it to make sure it matches the settings on the screenshot nonetheless.

1. Create IKE and VPN policies on your router using VPN Wizard.
2. Delete the VPN Policy, leaving the IKE policy.
3. Create new record for Mode Config in the following way:



Note: IP address ranges defined in: First, Second and Third Pool should be different then router's own LAN IP address range.

4. Modify your IKE Policy according to the following settings: